EXHIBIT 3

[bitcoin-dev] Taro: A Taproot Asset Representation Overlay

Olaoluwa Osuntokun laolu32 at gmail.com
Tue Apr 5 15:06:03 UTC 2022

- Previous message: [bitcoin-dev] BIP proposal: Pay-to-contract tweak fields for PSBT (bip-psbt-p2c)
- Next message: [bitcoin-dev] Taro: A Taproot Asset Representation Overlay
- **Messages sorted by:** [date] [thread] [subject] [author]

Hi y'all,

I'm excited to publicly publish a new protocol I've been working on over the past few months: Taro. Taro is a Taproot Asset Representation Overlay which allows the issuance of normal and also collectible assets on the main Bitcoin chain. Taro uses the Taproot script tree to commit extra asset structured meta data based on a hybrid merkle tree I call a Merkle Sum Sparse Merkle Tree or MS-SMT. An MS-SMT combined the properties of a merkle sum tree, with a sparse merkle tree, enabling things like easily verifiable asset supply proofs and also efficient proofs of non existence (eg: you prove to me you're no longer committing to the 1-of-1 holographic beefzard card during our swap). Taro asset transfers are then embedded in a virtual/overlay transaction graph which uses a chain of asset witnesses to provably track the transfer of assets across taproot outputs. Taro also has a scripting system, which allows for programmatic unlocking/transfer of assets. In the first version, the scripting system is actually a recursive instance of the Bitcoin Script Taproot VM, meaning anything that can be expressed in the latest version of Script can be expressed in the Taro scripting system. Future versions of the scripting system can introduce new functionality on the Taro layer, like covenants or other updates.

The Taro design also supports integration with the Lightning Network (BOLTs) as the scripting system can be used to emulate the existing HTLC structure, which allows for multi-hop transfers of Taro assets. Rather than modify the internal network, the protocol proposes to instead only recognize "assets at the edges", which means that only the sender+receiver actually need to know about and validate the assets. This deployment route means that we don't need to build up an entirely new network and liquidity for each asset. Instead, all asset transfers will utilize the Bitcoin backbone of the Lightning Network, which means that the internal routers just see Bitcoin transfers as normal, and don't even know about assets at the edges. As a result, increased demand for transfers of these assets as the edges (say like a USD stablecoin), which in will turn generate increased demand of LN capacity, result in more transfers, and also more routing revenue for the Bitcoin backbone nodes.

The set of BIPs are a multi-part suite, with the following breakdown:
 * The main Taro protocol:
https://github.com/Roasbeef/bips/blob/bip-taro/bip-taro.mediawiki
 * The MS-SMT structure:
https://github.com/Roasbeef/bips/blob/bip-taro/bip-taro-ms-smt.mediawiki
 * The Taro VM:
https://github.com/Roasbeef/bips/blob/bip-taro/bip-taro-vm.mediawiki
 * The Taro address format:
https://github.com/Roasbeef/bips/blob/bip-taro/bip-taro-addr.mediawiki
 * The Taro Universe concept:
https://github.com/Roasbeef/bips/blob/bip-taro/bip-taro-universe.mediawiki
 * The Taro flat file proof format:
https://github.com/Roasbeef/bips/blob/bip-taro/bip-taro-proof-file.mediawiki

Rather than post them all in line (as the text wouldn't fit in the allowed size limit), all the BIPs can be found above.

-- Laolu
-------------- next part --------------
An HTML attachment was scrubbed...
URL: <http://lists.linuxfoundation.org/pipermail/bitcoin-dev/attachments/20220405/930b239c/attachment.html>

- Previous message: [bitcoin-dev] BIP proposal: Pay-to-contract tweak fields for PSBT (bip-psbt-p2c)
- Next message: [bitcoin-dev] Taro: A Taproot Asset Representation Overlay
- **Messages sorted by:** [date] [thread] [subject] [author]

More information about the bitcoin-dev mailing list